

REMARKS:

This paper is herewith filed in response to the Examiner's Office Action mailed on February 27, 2009 for the above-captioned U.S. Patent Application. This office action is a rejection of claims 1-11 of the application.

More specifically, the Examiner has rejected claims 1, 4, and 6 under 35 USC 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention; objected to claim 1 because of informalities; rejected claims 1, 4-5, 7, and 9-11 under 35 USC 103(a) as allegedly "being anticipated" by Relander (US20020066012) in view of MacInnis (US5,951,1639); and rejected claims 2-3, 6, and 8 under 35 USC 103(a) as being unpatentable over Relander in view of MacInnis and in further view of Papineau (US7,092,703). The Applicant respectfully disagrees with the rejection.

Claims 1, 4-9, and 11 have been amended for clarification. Claims 1, 4 and 6 have been amended to address formalities. Support for the amendments can be found at least in paragraphs [0048], [0051], and [0053]. No new matter is added.

Regarding the rejections of claims 1, 4, and 6 under 35 USC 112, second paragraph, the rejections are addressed as follows:

In the rejection where the Examiner cites language in line 4 of claim 1, the Applicant notes that here "a dataflow" has been changed to "the dataflow."

In the rejection where the Examiner cites language in line 10 of claim 1, the Applicant notes that phrase "decrypt the encryption with" has been replaced with "decrypt the encrypted dataflow."

In the rejection where the Examiner cites language in lines 19-20 of claim 1, the Applicant notes that the applications referred to are the encryption applications being downloaded from the special server terminal device to the terminal equipment. The module referred in lines 12-13

S.N.: 10/511,934
Art Unit: 2432

comprises functionalities relating to synchronization (e.g. Synch Control 33.1 and Synch Detect 33.2). Further, the Applicant submits that this distinction is seen to be clear in claim 1 as amended.

In the rejection where the Examiner cites language in line 15 of claim 1, the Applicant notes that the “insufficient antecedent basis,” as indicated by the Examiner, has been addressed.

Regarding the rejection of claim 4 under 35 USC 112, second paragraph, the Applicant submits that there is seen to be sufficient antecedent basis in claim 1 for where claim 4 recites in part “wherein the downloading of the encryption applications and the encryption parameters.” This is seen to be the case for at least the reason that amended claim 1 recites in part “where terminal equipment is configured to download the encryption applications and encryption parameters.”

Regarding the rejection of claim 6 under 35 USC 112, second paragraph, the Applicant submits that claim 6, as amended, is seen to overcome the rejection.

The Applicant submits that, for at least these reasons, the rejection of claims 1, 4, and 6 under 35 USC 112, second paragraph, is seen to be overcome and the rejection should be removed.

In regards to section 10 of the Office action where the Examiner objects to claim 1 because of informalities, the Applicant respectfully notes that the Applicant is his own lexicographer. Thus, the Applicant does not wish to change the particular language of claim 1 as suggested by the Examiner. The Applicant respectfully submits that the phrase “de-synchronize the synchronization,” as identified by the Examiner in the objection, is appropriate for at least the reason that this phrase is seen to relate to a cancellation of the synchronization. The Applicant respectfully requests that for at least this reason the Examiner remove the objection.

Regarding the rejection of 1, 4-5, 7, and 9-11 under 35 USC 103(a), the Applicant disagrees with the Examiner.

As amended, claim 1 recites:

“A system comprising: a plurality of terminal equipment configured to communicate with one another using end-to-end encryption, where at least one of the plurality of terminal equipment functions as a special server terminal device configured to manage and distribute encryption applications and encryption parameters based on an established criterion to other pieces of the plurality of terminal equipment, where the encryption applications and encryption parameters are used during the end-to-end encryption, and where each of said plurality of terminal equipment comprises: a codec configured to convert an audio signal into a dataflow and vice versa, where the terminal equipment is configured to download the encryption applications and encryption parameters from said special terminal device via at least one interface, said terminal equipment further comprising a module configured to manage the download of the encryption applications and encryption parameters, an encryption key stream generator configured to generate a key stream segment with said encryption parameters, a processor configured to encrypt a the dataflow and decrypt the encrypted dataflow with the generated key stream segment, wherein a the module is configured to synchronize the encrypted dataflow and to de-synchronize the synchronization.”

The Applicant submits that the amendments provide further clarification of encryption parameters and an encryption procedure as indicated in claim 1. The Applicant submits that these amendments are seen to overcome the objections by the Examiner concerning indefiniteness. In addition, the Applicant notes that amendments remove a previously recited element of claim 1 related to synchronization applications being downloaded from the special server terminal device. The Applicant submits the amendment is supported for at least the reason that, as indicated in the specification, the terminal equipment may perform the synchronization by its own means.

In the rejection of claim 1 the Examiner states:

“Even though Relander teaches having the key stream generator and the synchronization control as part of the system in the form of hardware components or applications pre-installed in the system and that both are equivalent to and perform the functionality of encryption and synchronization applications of the current claimed invention, Relander does not explicitly teaches that the terminal equipment is configured to download said applications from said terminal device. MacInnis teaches that the terminal equipment is configured to download said applications from said terminal device [abstract and col 2 lines 18-52],” and

“At the time of the invention was made, it would have been obvious to an ordinary skill in the art to download to the terminal equipment (such as a cell phone) the needed software/applications/modules to be able to communicate (encrypt/decrypt/ synchronize) with the other terminal over the network [MacInnis, coil lines 6-15].”

Here, the Examiner states that “Relander does not explicitly [teach] that the terminal equipment is configured to download said applications from said terminal device.” Further, the Applicant notes that to overcome this admitted shortfall the Examiner cites MacInnis. The Applicant disagrees with the Examiner. The Applicant contends that a person of ordinary skill in the art clearly would not be motivated to combine Relander and MacInnis in order to arrive at the subject matter claimed in claim 1.

First, the Applicant notes that claim 1 relates to a plurality of terminal equipment configured to **communicate with one another using end-to-end encryption, where at least one of the plurality of terminal equipment functions as a special server terminal device** configured to manage and distribute encryption applications and encryption parameters. Whereas, MacInnis explicitly discloses that “The system, avoids the need for two-way communication between each terminal and the downloading source,” (Abstract). MacInnis discloses:

“One possible method for solving the aforementioned problem is to provide each terminal with means for requesting only a particular version of a module from the headend. **Unfortunately, such a scheme requires two-way communication between the terminals and the headend, which may be expensive and inefficient to provide, particularly since each terminal would require, at least temporarily, a dedicated channel for transmitting the requested version of the software or data,**” (emphasis added), (col. 1, lines 41-50); and

Here, MacInnis is seen to provide motivation for a method which does not require two-way communication between terminals and the headend. The Applicant notes that according to claim 1 there is a plurality of terminal equipment **communicating with one another**. Further, according to claim 1 at least one of the plurality of terminal equipment is configured to function as the special server terminal device. Thus, the Examiner imputing a server of MacInnis to be one

device of the plurality of the terminal equipment, which is configured to function as the special server terminal device, is clearly improper. This is the case for at least the reason, as stated above, that MacInnis can not be seen to disclose or suggest where claim 1 relates to **a device of a plurality of terminal equipment configured to communicate with one another** using end-to-end encryption, where at least one device is configured to function as the special server terminal device.

MacInnis discloses:

“However, as noted above, in networks such as subscription television systems, such two-way communication may be expensive and difficult to provide, and may result in increased complexity and reduced download performance. Furthermore, it may be difficult to coordinate version numbers among different software applications, complicating the task of determining which versions of complementary software should be downloaded into a particular terminal,” (col. 1, lines 57-65).

As indicated above, MacInnis again makes clear that two-way communication is undesirable.

The Applicant submits that MacInnis solution is related to downloading different versions of software or data modules **without requiring two-way client-server communication**. The Applicant notes that MacInnis relates to a cable television network, and the terminals into which software is downloaded are home communication terminals in the cable television network (col. 1 l. 6-9). Further, the Applicant submits that MacInnis discloses that any such two-way communication would be expensive and inefficient, and to provide a two-way communication for each terminal would require a dedicated channel for transmitting the requested version of the software or data (col. 1, lines 41-50). Therefore, the Applicant argues that the method of MacInnis is particularly targeted to **one-way communication** between a terminal and a server. Moreover, the Applicant contends that, for at least the reasons already stated, MacInnis is seen to teach away from a scheme that requires two-way communication.

The Applicant submits that for at least the reason that, as stated above, MacInnis is seen to disclose only one-way communication and to teach away from two-way communication,

MacInnis can not be seen to disclose or suggest a system comprising **a plurality of terminal equipment configured to communicate with one another using end-to-end encryption, where at least one of the plurality of terminal equipment functions as a special server terminal device** configured to manage and distribute encryption applications and encryption parameters based on an established criterion to other pieces of the plurality of terminal equipment, as in claim 1. More specifically, for at least this reason MacInnis clearly can not be seen to disclose or suggest at least the special server terminal of claim 1, as is applied by the Examiner in the rejection. Thus, for at least these reasons the rejection of claim 1 is seen to be improper and the rejection should be removed.

In addition, the Applicant submits that the cable television network of MacInnis and the TETRA communication system are not seen to be technically corresponding. Therefore, the Applicant contends that a person of ordinary skill in the art would not be motivated to implement MacInnis in order to solve a problem relating to encryption in TETRA-system. The Applicant submits that the proposed combination of Relander and MacInnis would not provide a system where part of the encryption components are outsourced (to special server terminal device), but where the encryption itself is maintained in the terminal as usual, as appears indicated in the rejection.

The Applicant contends that, for at least these reasons, a person of ordinary skill in the art would not be motivated to combine Relander and MacInnis. Although the Applicant does not agree that the proposed combination is proper, the Applicant submits that the proposed combination would, for at least the reasons already stated, still fail to disclose or suggest at least where claim 1 recites in part:

“A system comprising: a plurality of terminal equipment configured to communicate with one another using end-to-end encryption, where at least one of the plurality of terminal equipment functions as a special server terminal device configured to manage and distribute encryption applications and encryption parameters based on an established criterion to other pieces of the plurality of terminal equipment, where the encryption applications and encryption parameters are used during the end-to-end encryption”

S.N.: 10/511,934
Art Unit: 2432

The Applicant submits that for at least this reason the rejection of claim 1 is seen to be improper and the rejection should be removed.

Further, the Applicant submits that MacInnis discloses a requirement that a terminal device must retrieve a table T from the network to “extract information therefrom to determine which modules are compatible with the terminal,” (col. 6, lines 17-18). Further, MacInnis discloses that the terminal also include an internal table on the terminal to indicate how the terminal is configured as being manufactured (e.g. compatibility requirements). The Applicant submits that these features of MacInnis are seen to be derived from motivation relating to where MacInnis teaches away from two-way communication, as stated above.

According to MacInnis, as an example, a download mechanism of the terminal first extracts the table T and locates the different versions of a game listed in the table T which the user of the terminal wishes to download. The terminal of MacInnis then compares each of the different versions to the compatibility requirements and hardware requirements of the terminal and then determines which of the versions can be downloaded. The Applicant notes that Relander does not disclose or suggest any such table T or the internal table that appears required by MacInnis for the download. The Applicant contends that the proposed combination of Relander and MacInnis would at least require that new **inventive steps**, as stated above, be imposed in the terminal equipment of Relander. The Applicant argues that for at least this reason the proposed combination of Relander and MacInnis is seen to be improper and the rejection should be removed.

The Applicant contends that for at least the reasons stated the rejection of claim 1 is improper and the rejection should be removed.

Further, the Applicant submits that, for at least the reasons stated, the references cited can not be seen to disclose or suggest at least where independent claim 5 recites in part:

“a module is configured to receive and manage at least encryption keys, and

where **the apparatus is configured to download encryption applications and encryption parameters** via at least one interface, wherein at least one of said functionalities to **carry out end-to-end encrypted communication with another apparatus** is implemented using the encryption applications and the encryption parameters at a software level”

Thus, the rejection of claim 5 is seen to be improper and the rejection should be removed.

In addition, for at least the reasons already stated the references cited can not be seen to disclose or suggest at least where independent claim 7 recites in part:

“receiving from a data communication network information comprising at least one of encryption applications and encryption parameters comprising at least one encryption key; and executing the at least one of encryption applications and the encryption parameters to control the operation of a terminal equipment in order to **implement secure end-to-end data communication with another terminal equipment** using the at least one encryption key”

The applicant submits that for at least these reasons the rejection of claim 7 is seen to be improper and the rejection should be removed.

Further, the Applicant submits that, for at least the reasons already stated, the references cited can not be seen to disclose or suggest at least where independent claim 11 recites in part:

“managing at least one of encryption applications and encryption parameters concerning a data communication network; and **distributing the at least one of encryption applications and the encryption parameters based on an established criterion to pieces of terminal equipment**”

Thus, the references cited can not be seen to disclose or suggest claim 11 and the rejection should be removed.

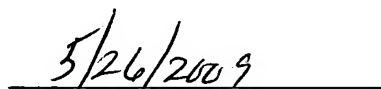
In addition, for at least the reason that claims 2-4, 6, and 8-10 depend from claims 1, 5, and 7 the references cited are not seen to disclose or suggest these claims.

S.N.: 10/511,934
Art Unit: 2432

Based on the above explanations and arguments, it is clear that the references cited cannot be seen to disclose or suggest claims 1-11. The Examiner is respectfully requested to reconsider and remove the rejections of claims 1-11 and to allow all of the pending claims 1-11 as now presented for examination.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record. Should any unresolved issue remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted:


John A. Garrity
Date

Reg. No.: 60,470

Customer No.: 29683

HARRINGTON & SMITH, PC

4 Research Drive

Shelton, CT 06484-6212

Telephone: (203)925-9400

Facsimile: (203)944-0245

email: jgarrity@hspatent.com

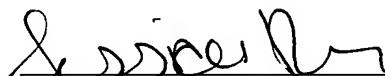
S.N.: 10/511,934
Art Unit: 2432

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

5.26.2009

Date



Name of Person Making Deposit